UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,192	12/02/2003	Simon Robert Walmsley	PEA17US	4559

24011 7590 02/01/2008

SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
02/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,192	WALMSLEY ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/ amendments with respect to amended claims 1 & 5 and previously presented claims 2-4 & 6-32 filed 11/28/2007 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Argument

Applicants contend that Spies et al. fails to teach "the subject matter of amended independent claim 1 and claims 2-32 dependent therefrom." Examiner respectfully disagrees. Spies et al. teach that the signature of the primary entity (i.e. trusted certificate authority) is used to hash the credentials (i.e. second secret information) submitted by one or more secondary entities (i.e. participants) by using the primary entity's first secret information (i.e. private key of the trusted certificate authority) in col. 11, lines 1-20. The amendment filed calls for "determining second secret information, such that the second secret information is a variant of the first secret information only ascertainable with knowledge of the first secret information." Keeping this limitation in mind, the credentials submitted by each of the participants are signed by using the trusted certificate authority's private key and hash function to create a signed credential where this concept constitutes the second secret information being a variant of the first secret information, where that signed credential can not be ascertained if the first secret information is not known. Thus, Spies et al. teach the subject matter of amended independent claim 1.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Foreign Priority

Acknowledgment is made of applicant's claim for foreign priority (filed with this amendment on 11/28/2007) based on applications filed in Australia on 12/2/2002. It is still noted, however, that **Applicant has not filed a proper certified copy of the actual/original foreign application as required by 35 U.S.C. 119(b)**. Specifically, **Applicants have submitted only a *provisional application/specification*** in connection with Applications 2002953134 and 2002953135 and not the actual foreign applications for patent which is necessary as required by 35 USC 119(a):

"An application for patent for an invention filed in this country by any person who has, or whose legal representatives or assigns have, previously regularly filed an application for a patent for the same invention in a foreign country which affords similar privileges in the case of applications filed in the United States or to citizens of the United States, or in a WTO member country, shall have the same effect as the same application would have if filed in this country on the date on which the application for patent for the same invention was first filed in such foreign country, if the application in this country is filed within twelve months from the earliest date on which such foreign application was filed; but no patent shall be granted on any application for patent for an invention which had been patented or described in a printed publication in any country more than one year before the date of the actual filing of the application in this country, or which had been in public use or on sale in this country more than one year prior to such filing."

Thus, until the proper certified copy of the foreign application for patent is filed, the foreign priority date claimed by the Applicants will not be used in determining the earliest effective filing date of the present application.

Claim Rejections - 35 USC § 102

I. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

II. Claims 1-4, 6-16, 18-20, 22-24, 26-28, and 30-32 are rejected under 35 U.S.C. 102(b) as being fully anticipated by Spies et al., US Patent No. 5,689,565.

As per claim 1:

Spies et al. teach a method including the steps of: allocating first secret information to the primary entity (col. 5, lines 3-6 and col. 6, lines 54-57); for each of the one or more secondary entities, determining second secret information by applying a one way function to that secondary entity's identifier and the first secret information (col. 6, lines 39-59), such that the second secret information is a variant of the first secret information only ascertainable with knowledge of the first secret information (col. 6, lines 49-59 and col. 11, lines 1-20); allocating the second secret information to the or each secondary entity (col. 6, lines 49-54).

As per claim 2:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach wherein the identifiers allocated to the secondary entities are generated stochastically, pseudo-randomly or arbitrarily (col. 9, lines 30-36).

As per claim 3:

Spies et al. teach the method according to claim 2. Furthermore, Spies et al. teach wherein the one-way function is a hash function (col. 6, lines 54-57).

As per claim 4:

Spies et al. teach the method according to claim 3. Furthermore, Spies et al. teach wherein the first secret information is a key (col. 5, lines 3-6).

As per claim 6:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach wherein each of the entities is implemented in an integrated circuit (col. 10, lines 10-24).

As per claim 7:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach wherein each of the entities is implemented in an integrated circuit separate from the integrated circuits in which the other entities are implemented (col. 10, lines 10-24).

As per claim 8:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach wherein one or more of the secondary entities are implemented in a corresponding plurality of integrated circuits (Fig. 1, elements 21(a-c) and col. 10, lines 10-24).

As per claim 9:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach wherein the primary entity is implemented in an integrated circuit (Fig. 1, elements 26 & 28 and col. 10, lines 10-24).

As per claim 10:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach wherein both the primary and secondary entities are implemented in integrated circuits (Fig. 1, elements 21(a-c), 26, & 28 and col. 10, lines 10-24).

As per claim 11:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach in which the first entity wishes to communicate with one of the second entities, the method including the steps, in the first entity, of: receiving data from the second entity (col. 6, lines 36-49); using the data and the first secret information to generate the second secret information associated with the second entity (col. 6, lines 49-57).

As per claim 12:

Spies et al. teach the method according to claim 11. Furthermore, Spies et al. teach wherein the data contains an identifier for the second entity (col. 8, lines 25-28).

As per claim 13:

Spies et al. teach the method according to claim 11. Furthermore, Spies et al. teach in which the first entity wishes to send an authenticated message to the second entity, the method including the steps, in the first entity, of: using the generated second secret information to sign a message, thereby generating a digital signature; outputting the message and the digital signature for use by the second entity, which can validate the message by using the digital signature and its own copy of the second secret information (col. 10, lines 2-17 and col. 11, lines 1-20).

As per claim 14:

Spies et al. teach the method according to claim 13. Spies further teach the method in which the generated signature includes its own copy of the second secret information (col. 10,

line 61 – col. 11, line 6) and in which the generated signature includes a nonce from the first entity, and the output from the first entity includes the nonce, thereby enabling the second entity to validate the message using the digital signature, the nonce (col. 9, lines 30-67).

As per claim 15:

Spies et al. teach the method according to claim 11. Furthermore, Spies et al. teach wherein the data contains a first nonce (col. 9, lines 30-36).

As per claim 16:

Spies et al. teach the method according to claim 15. Furthermore, Spies et al. teach the method in which the first entity wishes to send an authenticated message to the second entity, the method including the steps, in the first entity, of: using the generated second secret information and the nonce to sign a message (col. 9, lines 30-67), thereby generating a digital signature (col. 10, lines 2-17); outputting the message and the digital signature for use by the second entity, which can validate the message by using the digital signature and its own copy of the second secret information (col. 11, lines 1-20).

As per claim 18:

Spies et al. teach the method according to claim 11. Furthermore, Spies et al. teach the method in which the first entity wishes to send an encrypted message to the second entity, the method including the steps, in the first entity, of: using the generated second secret information to encrypt a message, thereby generating an encrypted message; outputting the encrypted message for use by the second entity, which can decrypt the message by using its own copy of the second secret information (col. 10, lines 2-24).

As per claim 19:

Spies et al. teach the method according to claim 18. Furthermore, Spies et al. teach the method in which the encrypted message includes a nonce from the first entity, and the output from the first entity includes the nonce, thereby enabling the second entity to decrypt the message using the nonce, and its own copy of the second secret information (col. 9, line 30 – col. 10, line 17).

As per claim 20:

Spies et al. teach the method according to claim 15. Furthermore, Spies et al. teach the method in which the first entity wishes to send an encrypted message that incorporates the first nonce to the second entity, the method including the steps, in the first entity, of: using the generated second secret information to encrypt a message and the first nonce, thereby generating an encrypted message; outputting the encrypted message for use by the second entity, which can decrypt the encrypted message by using its own copy of the second secret information (col. 9, line 30 – col. 10, line 17).

As per claim 22:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: using the second secret information to sign a message, thereby to generate a digital signature; and outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the

digital signature (col. 9, line 30 – col. 10, line 17 and col. 11, lines 52-67).

As per claim 23:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: using the second secret information and a nonce (col. 9, lines 30-36) to sign a message, thereby to generate a digital signature; and outputting the message, nonce, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the nonce and digital signature (col. 9, line 30 – col. 10, line 17 and col. 11, lines 52-67).

As per claim 24:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: receiving a first nonce from the first entity; using the second secret information and the first nonce (col. 9, lines 30-36) to sign a message, thereby to generate a digital signature; and outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the first nonce and digital signature (col. 9, line 30 – col. 10, line 17 and col. 11, lines 52-67).

As per claim 26:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: using the second secret information to encrypt the message, thereby to generate an encrypted message; and outputting the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message (col. 9, line 30 – col. 10, line 17).

As per claim 27:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: using the second secret information to encrypt the message and a nonce, thereby to generate an encrypted message; and outputting the nonce (col. 9, lines 30-36), encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message (col. 9, line 37 – col. 10, line 17).

As per claim 28:

Spies et al. teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: receiving a nonce from the first entity (col. 9, lines 30-36); using the second secret information to encrypt the message and the

nonce, thereby to generate an encrypted message; and outputting the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message (col. 9, line 37 – col. 10, line 17).

As per claim 30:

Spies et al. teach the method according to any one of claims 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 27, 28 or 29 (i.e. claim 14). Furthermore, Spies et al. teach wherein at least one of the nonces is a pseudo-random number (col. 9, lines 30-36).

As per claim 31:

Spies et al. teach the method according to any one of claims 11 to 21 (i.e. claim 11). Furthermore, Spies et al. teach wherein the communication is an authenticated read of a field of the first entity (col. 10, lines 10-24).

As per claim 32:

Spies et al. teach the method according to any one of claims 22 to 29 (i.e. claim 22). Furthermore, Spies et al. teach wherein the communication is an authenticated read of a field of the second entity (col. 10, lines 10-24).

Claim Rejections - 35 USC § 103

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

IV. Claims 5, 17, 21, 25, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al., US Patent No. 5,689,565 as applied to claims 1, 3, 16, and 20 above, and further in view of Bruce Schneier, *Applied Cryptography.*

As per claim 5:

Spies et al. substantially teach the method according to claim 3. Not explicitly disclosed is wherein the one-way function is a Secure Hash Algorithm function. However, Schneier teaches that using SHA ensure the security of the Digital Signature Algorithm. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Spies et al. to use SHA as the one-way hash function utilized in creating the digital signature. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that SHA is secure since it is computationally infeasible to recover a message corresponding to a particular message digest on page 442, second paragraph under section 18.7.

As per claim 17:

Spies et al. substantially teach the method according to claim 16. Not explicitly disclosed is the method in which the generated signature includes a second nonce from the first entity, and the output from the first entity includes the second nonce, thereby enabling the second entity to validate the message using the digital signature, the first and second nonces, and its own copy of the second secret information. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Spies et al. to use timestamps with digital signature technology in order to prevent

from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."

As per claim 21:

Spies et al. substantially teach the method according to claim 20. Not explicitly disclosed is the method in which the encrypted message includes a second nonce from the first entity, and the output from the first entity includes the second nonce. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Spies et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."

As per claim 25:

Spies et al. substantially teach the method according to claim 1. Furthermore, Spies et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: receiving a first nonce from the first entity; using the second secret information and the first nonce, thereby to generate a digital signature; and outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret

information to generate the second secret information associated with the second entity, and thereby authenticate the message via the first nonce, and digital signature (col. 9, line 30 – col. 10, line 17 and col. 11, lines 52-67).

Not explicitly disclosed is using a second nonce in generating a signature for the message, outputting the second nonce, and authenticating the second nonce. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Spies et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."
As per claim 29:

Spies et al. substantially teach method according to claim 1. Furthermore, Spies et in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: receiving a first nonce from the first entity; using the second secret information to encrypt the message and the first nonce, thereby to generate an encrypted message; and outputting, the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message (col. 9, line 30 – col. 10, line 17).

Not explicitly disclosed is encrypting a second nonce and outputting a second nonce. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Spies et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Nadia Khoshnoodi
Examiner
Art Unit 2137
1/29/2008

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

NK

1/30/08